

A family of loss-tolerant quantum coin flipping protocols

N. Aharon¹, S. Massar² and J. Silman²

¹*School of Physics and Astronomy, Tel-Aviv University, Tel-Aviv 69978, Israel*

²*Laboratoire d'Information Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*

We present a family of loss-tolerant quantum strong coin flipping protocols; each protocol differing in the number of qubits employed. For a single qubit we obtain a bias of 0.4, reproducing the result of Berlín *et al.* [Phys. Rev. A **80, 062321 (2009)], while for two qubits we obtain a bias of 0.3975. Numerical evidence based on semi-definite programming indicates that the bias continues to decrease as the number of qubits is increased but at a rapidly decreasing rate.**

I. INTRODUCTION

Coin flipping (CF) is a cryptographic task in which a pair of remote distrustful parties, usually referred to as Alice and Bob, must agree on a random bit. The problem was first introduced in 1981 by Blum [1], who studied it in classical settings. There are two variants of the problem: ‘strong’ CF (SCF) and ‘weak’ CF (WCF). In SCF each party is not aware of the other’s preference for the coin’s outcome. In contrast, in WCF the parties have opposite and known preferences. Hence, in WCF there is always a winner and a loser, unless one of the parties is caught cheating, in which case the protocol is aborted. Let P_{xy} denote the probability that the Alice (Bob) obtains the outcome x (y) and let P_{\perp} denote the probability that the protocols is aborted. If both parties are honest then $P_{00} = P_{11} = 1/2$ and $P_{10} = P_{01} = P_{\perp} = 0$, i.e. the parties always agree on the outcome of the coin. The security of a CF protocol is quantified by the extent to which dishonest parties can bias the outcome. We denote by $P_{*i} \triangleq 1/2 + \epsilon_{*i}$ ($P_{i*} \triangleq 1/2 + \epsilon_{i*}$) the maximal probability of Alice (Bob) to bias the outcome to i . In SCF the bias is defined as $\epsilon \triangleq \max\{\epsilon_{*0}, \epsilon_{*1}, \epsilon_{0*}, \epsilon_{1*}\}$, while in WCF the maximum is taken over only two of the biases: If, for example, Alice prefers the outcome 0, then the bias equals $\max\{\epsilon_{*0}, \epsilon_{1*}\}$. A protocol is said to be fair whenever both parties enjoy the same bias.

In classical settings, given unlimited computational power, a dishonest party can always bias the outcome as it desires [2]. In contrast, this is not the case in quantum settings. Aharonov *et al.* formulated the first (non-trivial) quantum SCF protocol in 2000 [3]. This protocol, which achieves a bias of 0.354 [4], began the quest for a SCF protocol with a vanishing bias. First, Spekkens and Rudolph devised a protocol with a bias of 0.309 [4]. Ambainis [5] and independently Spekkens and Rudolph [6] soon afterwards introduced protocols pushing the bias to as low as $1/4$. However, the prospects of further progress were soon shadowed by two key results. Ambainis proved that any protocol with a bias of ϵ , whether strong or weak, must consist of at least $\Omega(\log \log \epsilon^{-1})$ rounds of communication [5], while Kitaev proved that the bias of any quantum SCF protocol is bounded by $(\sqrt{2} - 1)/2 \simeq 0.207$ [7]. Until recently, it was not known whether this bound can be saturated or whether the bias of $1/4$ is optimal. This point has now been settled by Chailloux and Kerenidis who have presented a protocol that saturates Kitaev’s bound [8], based on Mochon’s work proving the possibility of quantum WCF with arbitrarily small bias [9].

Quantum WCF was first analyzed by Spekkens and Rudolph in 2001, who introduced a family of protocols that achieves a bias of $(\sqrt{2} - 1)/2$ [10]. (Previously Goldenberg *et al.* analyzed the problem of quantum gambling [11], which is a closely related cryptographic task.) This result was subsequently improved upon by Mochon who considered WCF protocols with an infinite number of rounds [12, 13], eventually culminating in the aforementioned result [9]. In addition, quantum SCF and WCF have also been studied in the multi-party [14] multi-outcome scenario [15, 16] and most recently in both [17, 18].

Even though from a purely theoretical viewpoint a lot of progress has been made in our understanding of quantum CF, most quantum CF protocols are impractical due to the non-ideal conditions prevalent in any real-life implementation. These include uncertainties in the preparation and measurement of states, whether inherent or due to noise, as well as noise and losses in the quantum channels and the quantum memory storage. In the sending of quantum information over long distances the most common source of malfunctions is losses. The problem with losses is that they introduce a finite probability for an indefinite outcome – actually no outcome at all – even when both parties are honest, so that there is always a non-vanishing chance for the protocol to be aborted (i.e. $P_{\perp} = 1 - P_{00} - P_{11} > 0$). As pointed out in [15], one way to avoid this situation, is to restart the protocol each time an indefinite outcome occurs, but this in turn affords a dishonest party very simple cheating strategies, which may even go so far as to enable it to bias the outcome to its choosing. Remarkably, Berlín *et al.* have recently devised a ‘loss-tolerant’ SCF protocol [19, 20] (see also [21]). That is, a protocol whose bias remains unchanged even if we allow for the protocol to be restarted. However, the loss-tolerance came at a price: the protocol achieves a comparatively high bias of 0.4.

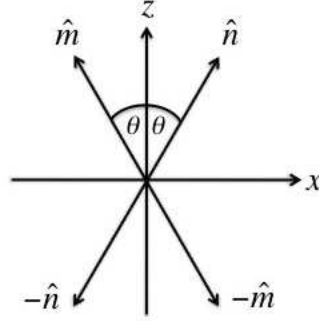


Figure 1: Alice's preparation. Each qubit that Alice prepares is polarized along one of the four axes $\pm\hat{n}$ and $\pm\hat{m}$.

It may well be that there is always a price to be paid. Specifically, it could be that loss-tolerant SCF cannot saturate Kitaev's bound. Indeed, at the end of their paper Berlín *et al.* raise the question of whether it is possible to devise a loss-tolerant protocol with a lower bias than theirs.

In this paper we answer this question in the affirmative by introducing a family of loss-tolerant SCF protocols, which outperforms Berlín *et al.*'s protocol. Each member in the family differs in the number of qubits employed. In the one qubit case we achieve the same bias as Berlín *et al.*, $\epsilon = 0.4$, while for two qubits the bias reduces to 0.3975. Numerical evidence based on semi-definite programming [23] suggests that the bias continues to decrease as the number of qubits is increased, but at a rapidly decreasing rate. Our protocol bears some similarity to the original BB84 CF protocol [22] and its various derivatives [3, 5, 19], but significantly differs in that it is not based on bit-commitment.

II. A FAMILY OF LOSS-TOLERANT PROTOCOLS

The protocols read as follows:

1. Alice selects N orientations $\hat{\alpha}_1$ to $\hat{\alpha}_N$, where each of the $\hat{\alpha}_i$ is (uniformly) randomly picked from a set of four predetermined orientations \hat{n} , $-\hat{n}$, \hat{m} , and $-\hat{m}$ (which are known to Bob). Alice prepares N qubits polarized along these orientations, i.e. the first qubit is polarized along $\hat{\alpha}_1$, the second along $\hat{\alpha}_2$, etc., and sends these N qubits to Bob.
2. Bob selects N orientations $\hat{\beta}_1$ to $\hat{\beta}_N$, where each of the $\hat{\beta}_i$ is (uniformly) randomly picked from the set of two orientations \hat{n} and \hat{m} , and then measures the polarization of the first qubit along $\hat{\beta}_1$, the polarization of the second along $\hat{\beta}_2$, etc.
3. If all the measurements are successful (i.e. he has detected the N qubits and has obtained N definite outcomes), he asks Alice to proceed with the protocol, otherwise, he asks her to restart the protocol (i.e. repeat step 1).
4. Alice sends Bob a randomly selected classical bit c .
5. Let r_1 to r_N denote the outcomes of Bob's N measurements. The outcome of the coin flip o is given by $o = c \oplus (\bigoplus_{i=1}^N r_i)$. Bob informs Alice of his choice of orientations, $\hat{\beta}_i$, and the corresponding outcomes, r_i .
6. Alice aborts whenever there is at least one qubit that Bob claims to have successfully measured for which $(1 - 2r)\hat{\beta} = -\hat{\alpha}$.

The loss tolerance of the protocol comes into play at step 3, where Bob asks Alice to restart the protocol whenever one or more of his measurements are unsuccessful, in which case the outcomes of the successful measurements are discarded. That is, Bob must successfully measure N -qubits in a single run of the protocol. Also note that we do not fix the angle between the axes \hat{n} and \hat{m} . Indeed, this angle is a free parameter. In particular, it turns out that by manipulating it we can make the protocol 'fair' in the sense that Alice's and Bob's maximal biases are equal.

III. ALICE'S MAXIMAL BIAS

It will prove convenient to choose the coordinate system such that \hat{n} and \hat{m} lie on the xz plane, spanning an angle of θ , $-\theta$, respectively, from the z axis (see Fig. 1).

Since Bob is honest he will measure each qubit along one of the two axes \hat{n} and \hat{m} with equal probability. Suppose that Alice wishes to bias the outcome to 0. With no loss of generality we assume that Alice selects $c = 0$. Then the probability that she is successful equals

$$P_{*0}^{(N)} = \max_{\rho} \frac{1}{2^N} \sum_{\hat{b}_1=\hat{n}, \hat{m}} \dots \sum_{\hat{b}_n=\hat{n}, \hat{m}} P\left(\bigoplus_{i=1}^N r_i = 0 \mid \{\hat{b}_1, \hat{b}_2, \dots, \hat{b}_N\}, \rho\right); \quad (1)$$

the superscript N serving to denote the number of qubits employed in the protocol. Introducing the operator

$$\Pi_N \hat{=} \frac{1}{2^N} \sum_{\hat{b}_1=\hat{n}, \hat{m}} \sum_{s_1=\pm 1} \dots \sum_{\hat{b}_n=\hat{n}, \hat{m}} \sum_{s_N=\pm 1} \Theta(s_1 \cdot s_2 \cdot \dots \cdot s_N) \bigotimes_{i=1}^N |\uparrow_{s_i \hat{b}_i}\rangle \langle \uparrow_{s_i \hat{b}_i}|, \quad (2)$$

where $\Theta(x)$ is the Heaviside step function, we have that

$$P_{*0}^{(N)} = \max_{\rho} \text{Tr}(\rho \Pi_N). \quad (3)$$

Clearly, the maximum obtains when ρ equals the (normalized) eigenvector (or any one of the eigenvectors) of Π_N corresponding to the greatest eigenvalue. Making use of the fact that

$$|\uparrow_{\pm \hat{n}}\rangle \langle \uparrow_{\pm \hat{n}}| + |\uparrow_{\pm \hat{m}}\rangle \langle \uparrow_{\pm \hat{m}}| = \mathbb{1} \pm \cos(\theta) \sigma_z \quad (4)$$

(and $s_1 \cdot s_2 \cdot \dots \cdot s_N = 1$ since Alice wishes to bias the outcome to 0), eq. (2) simplifies to

$$\begin{aligned} \Pi_N &= \frac{1}{2^N} \sum_{s_1=\pm 1} \dots \sum_{s_N=\pm 1} \Theta(s_1 \cdot s_2 \cdot \dots \cdot s_N) \bigotimes_{i=1}^N (\mathbb{1}_i + s_i \cos(\theta) \sigma_z^{(i)}) \\ &= \frac{1}{2^N} \sum_{s_1=\pm 1} \dots \sum_{s_N=\pm 1} \Theta(s_1 \cdot s_2 \cdot \dots \cdot s_N) \left(\mathbb{1} + \sum_{i=1}^N s_i \cos(\theta) \Sigma_z^{(i)} + 2 \sum_{i=1}^N \sum_{j=i+1}^N s_i s_j \cos^2(\theta) \Sigma_z^{(i)} \Sigma_z^{(j)} \right. \\ &\quad \left. + \dots + \cos^N(\theta) \prod_{i=1}^N \Sigma_z^{(i)} \right) \\ &= \frac{1}{2} \left(\mathbb{1} + \cos^N(\theta) \bigotimes_{i=1}^N \sigma_z^{(i)} \right). \end{aligned} \quad (5)$$

Here we use the notation

$$\Sigma_{\mathbf{a}}^{(i)} \hat{=} \mathbb{1}_1 \otimes \dots \otimes \mathbb{1}_{i-1} \otimes \sigma_z^{(i)} \otimes \mathbb{1}_{i+1} \otimes \dots \otimes \mathbb{1}_N, \quad \mathbf{a} = x, y, z \quad (6)$$

with $\mathbb{1}_i$ denoting the identity operator on the Hilbert space of the i th qubit. The eigenvalues of Π_N equal $(1 \pm \cos^N(\theta))/2$. The resulting biases are thus given by

$$P_{*0}^{(N)} = P_{*1}^{(N)} = \frac{1}{2} (1 + \cos^N(\theta)), \quad (7)$$

since the probability of biasing to 0 and 1 are patently equal.

IV. BOB'S MAXIMAL BIAS

In the following it will prove economical to employ the following notation: $|\psi_0^{(0)}\rangle \hat{=} |\uparrow_{\hat{n}}\rangle$, $|\psi_0^{(1)}\rangle \hat{=} |\downarrow_{\hat{n}}\rangle$, $|\psi_1^{(0)}\rangle \hat{=} |\uparrow_{\hat{m}}\rangle$, $|\psi_1^{(1)}\rangle \hat{=} |\downarrow_{\hat{m}}\rangle$, so that the basis $|\uparrow_{\hat{n}}\rangle, |\downarrow_{\hat{n}}\rangle$ ($|\uparrow_{\hat{m}}\rangle, |\downarrow_{\hat{m}}\rangle$) is denoted by 0 (1). In addition, we define $|\psi_{\mathbf{b}}^{(\mathbf{r})}\rangle \hat{=} \bigotimes_{i=1}^N |\psi_{b_i}^{(r_i)}\rangle$,

where $\mathbf{b} \triangleq (b_1, b_2, \dots, b_N)$ and $\mathbf{r} \triangleq (r_1, r_2, \dots, r_N)$ are binary N -tuples, i.e. $b_i, r_i \in \{0, 1\}$.

The loss-tolerant nature of the protocol allows (a dishonest) Bob to carry out a measurement at step 2 to decide whether to keep the N the qubits. Only when he has decided to keep them does he proceed to step 4. Then, depending on the value of the classical bit c (received at step 4), he will carry out another measurement on the N qubits at step 5. The outcome of this measurement instructs him what N -tuples \mathbf{b} and \mathbf{r} to tell Alice that he selected and (supposedly) obtained, respectively. More specifically, at step 2 Bob will carry out a two-outcome POVM with elements $\Pi_p, \Pi_{rs} = 1 - \Pi_p$. If he obtains the outcome associated with Π_{rs} he asks Alice to restart the protocol. Otherwise, if he obtains the outcome associated with Π_p , he keeps the qubits and they proceed to step 4. At step 5 Bob already knows the value of c . Let us assume that he would like to bias the outcome to 0, then to optimize his chances of being successful he will have to tell Alice announce an N -tuple \mathbf{r} such that $\bigoplus_i r_i = 0 \oplus c = c$. He will then carry out an additional POVM on the N -qubits with 2^{2N-1} outcomes, which instructs him what N -tuples \mathbf{b} and \mathbf{r} to announce. We will denote this second POVM by $\Pi_{0c}^{\mathbf{r}\mathbf{b}}$, where the subscripts 0 and c correspond to the value to which Bob wants to bias the coin and the value of the classical bit sent by Alice, and the superscripts \mathbf{b} and \mathbf{r} correspond to the choice of bases and the associated outcomes that he sends Alice. Hence, a cheating strategy designed to obtain the outcome 0 consists of a set of three POVMs with elements $\{\Pi_p, \Pi_{rs}\}$, $\{\Pi_{0c}^{\mathbf{r}\mathbf{b}} \mid \bigoplus_i r_i = 0\}$ and $\{\Pi_{0c}^{\mathbf{r}\mathbf{b}} \mid \bigoplus_i r_i = 1\}$.

In the following it will facilitate matters to introduce the positive operators $M_{0c}^{\mathbf{r}\mathbf{b}} \triangleq \sqrt{\Pi_p} \Pi_{0c}^{\mathbf{r}\mathbf{b}} \sqrt{\Pi_p}$, which we note satisfy

$$\sum_{\{\mathbf{b}\}} \sum_{\{\mathbf{r} \mid \bigoplus_i r_i = c\}} M_{0c}^{\mathbf{r}\mathbf{b}} = \sqrt{\Pi_p} \sum_{\{\mathbf{b}\}} \sum_{\{\mathbf{r} \mid \bigoplus_i r_i = c\}} \Pi_{0c}^{\mathbf{r}\mathbf{b}} \sqrt{\Pi_p} = \Pi_p. \quad (8)$$

Suppose now that Alice prepared at step 1 the state $|\psi_{\mathbf{a}}^{(s)}\rangle$, and, having been asked to proceed with the protocol, sends Bob the classical bit c at step 4. Bob gets caught cheating when for one or more of the qubits, $b_i = a_i$ and $r_i = s_i \oplus 1$. Bob's minimal probability of being caught cheating therefore equals

$$1 - P_{0*}^{(N)} = \frac{1}{2^{2N+1}} \min_{\{M_{0c}^{\mathbf{r}\mathbf{b}}\}} \sum_{c=0,1} \sum_{\{\mathbf{a}\}} \sum_{\{\mathbf{s}\}} \sum_{\{\mathbf{b}\}} \sum_{\{\mathbf{r} \mid \bigoplus_i r_i = c\}} \Theta\left(\sum_{j=1}^N \delta_{b_j, a_j} \cdot \delta_{r_j, s_j \oplus 1}\right) \frac{\langle \psi_{\mathbf{a}}^{(s)} | M_{0c}^{\mathbf{r}\mathbf{b}} | \psi_{\mathbf{a}}^{(s)} \rangle}{\langle \psi_{\mathbf{a}}^{(s)} | \Pi_p | \psi_{\mathbf{a}}^{(s)} \rangle}, \quad (9)$$

where the summation is carried out over the set of all possible binary N -tuples, $\{\mathbf{a}\}$, $\{\mathbf{b}\}$, $\{\mathbf{s}\}$, and $\{\mathbf{r} \mid \bigoplus_i r_i = c\}$. The Heaviside step-function, additionally defined such that $\Theta(0) \triangleq 0$, serves to guarantee that only terms, which satisfy $b_i = a_i$ and $r_i = s_i \oplus 1$ for at least one $i \in \{1, 2, \dots, n\}$, contribute. Finally, the 2^{2N+1} factor is just the number of possible choices for the triplet c, \mathbf{a} , and \mathbf{s} .

Clearly, no value of c is in any way preferable for Bob, nor is any orientation or any particular qubit. This implies the existence of an optimal symmetric cheating strategy in the sense that all of the POVM elements (pertaining to both the POVM carried out when $c = 0$ and the POVM carried out when $c = 1$) contribute equally. To see this, we first assume the existence of an optimal (possibly asymmetric) strategy. Let $\{\tilde{M}_{0c}^{\mathbf{r}\mathbf{b}}\}$ and $\{\tilde{M}_{0c}^{\mathbf{r}\mathbf{b}}\}$ denote the corresponding two sets of positive operators. Then, for any binary N -tuple \mathbf{u} , another optimal cheating strategy is obtained by the transformation

$$\tilde{M}_{0c}^{\mathbf{r}\mathbf{b}} \rightarrow M_{0c}^{\mathbf{r}\mathbf{b} \oplus \mathbf{u}} = \Sigma_z^{\mathbf{u}} \tilde{M}_{0c}^{\mathbf{r}\mathbf{b}} \Sigma_z^{\mathbf{u}}, \quad (10)$$

where $\Sigma_{\mathbf{a}}^{\mathbf{u}} \triangleq \prod_{i=1}^N \Sigma_{\mathbf{a}}^{(i) u_i}$ ($\mathbf{a} = x, y, z$) and $\mathbf{a} \oplus \mathbf{b} \triangleq (a_1 \oplus b_1, \dots, a_N \oplus b_N)$, corresponding to rotations by π about the z axes of the coordinate systems of the set of qubits $\{i \mid u_i = 1\}$. Similarly, for any binary N -tuple \mathbf{u} , we obtain yet another optimal cheating strategy via

$$\tilde{M}_{0c}^{\mathbf{r}\mathbf{b}} \rightarrow M_{0c \oplus (\bigoplus_i u_i)}^{\mathbf{r} \oplus \mathbf{u} \mathbf{b} \oplus \mathbf{u}} = \Sigma_x^{\mathbf{u}} \tilde{M}_{0c}^{\mathbf{r}\mathbf{b}} \Sigma_x^{\mathbf{u}}, \quad (11)$$

corresponding to rotations by π about the x axes of the coordinate systems of the set of qubits $\{i \mid u_i = 1\}$. (When $\bigoplus_i u_i = 1$ we switch from a POVM corresponding to one value of c to a POVM corresponding to the other value.)

Now a strategy in which Bob chooses at random between different optimal strategies is also optimal. By choosing uniformly at random between optimal strategies related by the transformations eqs. (10) and (11), Bob obtains an optimal strategy characterized by the positive operators

$$M_{0c}^{\mathbf{r}\mathbf{b}} = \frac{1}{4^N} \sum_{\{\mathbf{u}\}} \sum_{\{\mathbf{w}\}} \Sigma_x^{\mathbf{u}} \Sigma_z^{\mathbf{w}} \tilde{M}_{0c \oplus (\bigoplus_i u_i)}^{\mathbf{r} \oplus \mathbf{u} \mathbf{b} \oplus \mathbf{u}} \Sigma_x^{\mathbf{u}} \Sigma_z^{\mathbf{w}}; \quad (12)$$

the only subtle point in the above argument concerns those transformations given by eq. (11) that modify the value c and exchange between elements in $\{\tilde{M}_{00}^{\mathbf{r}\mathbf{b}}\}$ and $\{\tilde{M}_{01}^{\mathbf{r}\mathbf{b}}\}$. Nevertheless, this does not pose a problem since in an

optimal cheating strategy the overall contribution to the cheating probability when $c = 0$ and $c = 1$ must be equal, and, moreover, eqs. (11) and the invariance of Π_p under the application of the rotation operators, imply that in an optimal cheating strategy the sets $\{\tilde{M}_{00}^{\mathbf{r}\mathbf{b}}\}$ and $\{\tilde{M}_{01}^{\mathbf{r}\mathbf{b}}\}$ can be obtained from one another via the transformation eq. (11). Finally, we note that this pair of sets, eq. (12), can be characterized by any of the positive operators within the sets, say $M_{00}^{\mathbf{0}\mathbf{0}}$ ($\mathbf{0} \triangleq (0, \dots, 0)$). All other positive operators (including those corresponding to $c = 1$) can be obtained from it by the transformations eqs. (10) and (11). In appendix A we prove that eqs. (8), (10), (11) and (12) imply that one can take $\Pi_p = \mathbb{1}$. This means that Bob stands nothing to gain by performing a measurement on the qubits prior to receiving the value of the classical bit c .

The problem of optimizing Bob's bias can be cast as an SDP (see [23] for an introduction). Using the fact that we can set $\Pi_p = \mathbb{1}$ (and recalling that the rotation operators switch between all of Alices' preparations), the right-hand side of eq. (9) can be reexpressed as $\text{Tr}(M_{00}^{\mathbf{0}\mathbf{0}} \Lambda_N(\theta))$, with

$$\Lambda_N(\theta) = \frac{1}{2^{2N+1}} \sum_{c=0,1} \sum_{\{\mathbf{a}\}} \sum_{\{\mathbf{s}\}} \sum_{\{\mathbf{b}\}} \sum_{\{\mathbf{r} \oplus_i r_i = c\}} \Theta\left(\sum_{j=1}^N \delta_{b_j, a_j} \cdot \delta_{r_j, s_j \oplus 1}\right) |\psi_{\mathbf{a} \oplus \mathbf{b}}^{(\mathbf{s} \oplus \mathbf{r})}\rangle \langle \psi_{\mathbf{a} \oplus \mathbf{b}}^{(\mathbf{s} \oplus \mathbf{r})}|. \quad (13)$$

The SDP then reads

$$\begin{aligned} P_{0*}^{(N)} &= \max_{M_{00}^{\mathbf{0}\mathbf{0}}} (1 - \text{Tr}(M_{00}^{\mathbf{0}\mathbf{0}} \Lambda_N(\theta))) \\ \text{subject to} \quad & 2^{N-1} \text{Tr}(M_{00}^{\mathbf{0}\mathbf{0}}) = 1, \quad \text{Tr}(M_{00}^{\mathbf{0}\mathbf{0}} \otimes_{i=1}^N \sigma_z^{(i)}) = 0, \quad M_{00}^{\mathbf{0}\mathbf{0}} \geq 0. \end{aligned} \quad (14)$$

The derivation of the first two constraints is given in Appendix A.

Now problems of this type, have associated with them a dual problem. The solution of this dual problem bounds from above the solution of the original problem, [23], which we shall refer to as the 'primal' problem. It is given by

$$\begin{aligned} & \min_{\lambda_i} (1 - \tfrac{1}{2} \lambda_1) \\ \text{subject to} \quad & \Lambda_N(\theta) - \lambda_1 \mathbb{1} + \lambda_2 \otimes_{i=1}^N \sigma_z^{(i)} \geq 0, \end{aligned} \quad (15)$$

where the variables of the dual problem, the λ_i , are real scalars.

A. The single qubit case

It is straightforward to solve both eqs. (14) and (15) in the single qubit case. The solution is given by

$$P_{0*}^{(1)} = P_{1*}^{(1)} = \frac{1}{4} (3 + \sin(\theta)), \quad (16)$$

where the second equality follows from the equality of the probabilities of biasing to 0 and 1, and is obtained for $2M_{00}^{\mathbf{0}\mathbf{0}} = \mathbb{1} + \sigma_x$. Hence, Bob's strategy consists of measuring the polarization of the qubit along the x axis.

B. The two-qubit case

In the two qubit case Bob measures an eight outcome POVM $M_0^{(r_1, r_1 \oplus c)\mathbf{b}}$ (recall that we have assumed that Bob wants to bias the outcome to 0). By introducing a new set of Lagrange multipliers $\xi = \lambda_1 - \lambda_2$ and $\chi = \lambda_1 + \lambda_2$, the dual problem can be reexpressed as

$$\begin{aligned} & \min_{\xi, \chi} (1 - \tfrac{1}{4} (\xi + \chi)) \\ \text{subject to} \quad & \Lambda_2(\theta) - \xi (|\uparrow\uparrow\rangle \langle\uparrow\uparrow| + |\downarrow\downarrow\rangle \langle\downarrow\downarrow|) - \chi (|\uparrow\downarrow\rangle \langle\uparrow\downarrow| + |\downarrow\uparrow\rangle \langle\downarrow\uparrow|) \geq 0. \end{aligned} \quad (17)$$

The solution obtains when

$$\det(\Lambda_2(\theta) - \xi (|\uparrow\uparrow\rangle \langle\uparrow\uparrow| + |\downarrow\downarrow\rangle \langle\downarrow\downarrow|) - \chi (|\uparrow\downarrow\rangle \langle\uparrow\downarrow| + |\downarrow\uparrow\rangle \langle\downarrow\uparrow|)) = 0, \quad (18)$$

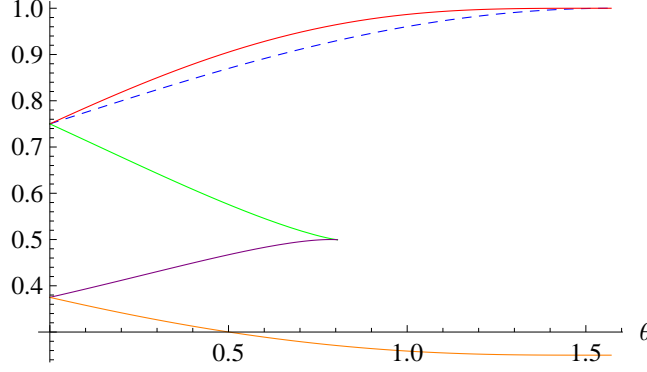


Figure 2: The dashed curve depicts Bob's maximal probability of biasing the outcome in the single qubit case, while each of the four other curves depict eq. (17) as a function of a different root of eq. (20). Note that two of the roots become complex beyond $\theta \simeq 0.8056$.

i.e. when the lowest eigenvalue of the constraint matrix eq. (17) equals zero. Solving for χ in terms of ξ we get

$$\chi = \frac{(\cos(2\theta) + 7)\xi^2 - 3(\cos(2\theta) + 3)\xi}{8\xi^2 + (\cos(2\theta) - 13)\xi - 3(\cos(2\theta) - 1)}. \quad (19)$$

(There is another solution $\chi = 1$, but it can be shown that in this case the constraint matrix always admits a negative eigenvalue.) Plugging back into eq. (17), taking the derivative with respect to ξ , and equating to zero, we get a fourth order equation in ξ

$$64\xi^4 + 16(\cos(2\theta) - 13)\xi^3 + (\cos(4\theta) - 56\cos(2\theta) + 199)\xi^2 - 6(\cos(4\theta) - 8\cos(2\theta) + 7)\xi + 9(\cos(4\theta) - 1) = 0. \quad (20)$$

When plugged back into eq. (17) three of the four roots do not give rise to expressions smaller to Bob's maximal bias in the single qubit case. See Fig. 2. Hence, none of these three represents a solution of the primal problem since its solution must bound above the solution of the dual problem and clearly Bob can always achieve a bias equal to that of the single qubit case by simply not following the directions of the protocol in the handling of only one of the qubits. It is straightforward to show that the remaining eigenvalue satisfies the constraints of the dual problem (i.e. all other three eigenvalues are positive), and therefore gives rise to an upper bound on Bob's maximal bias.

V. BIASES IN THE FAIR SCENARIO

To make the protocol fair, i.e. $P_F^{(N)} = P_{*i}^{(N)} = P_{j*}^{(N)}$, we have the freedom to manipulate θ . In this way, for a single qubit we obtain $P_{*i}^{(1)} = P_{j*}^{(1)} = 0.9$ ($\theta \simeq 36.87^\circ$). In the two qubit case, the solution of the dual problem and Alice's maximal bias intersect for $\theta \simeq 26.92^\circ$, $\xi \simeq -0.2098$, $\chi \simeq 0.6197$, $1 - (\xi + \chi)/4 \simeq P_{*0}^{(2)} \simeq 0.8975$. It remains to prove that this intersection indeed corresponds to Bob's maximal bias, or, what is the same thing, to show that for this value of the angle the solution of the dual problem coincides with that of the primal problem.

To do so we conjecture that the solution of the primal problem, eq. (15) in the case $N = 2$, is of the form

$$2M_{00}^{00} = |v(\theta)\rangle \langle v(\theta)|, \quad (21)$$

where

$$|v(\theta)\rangle = \frac{1}{\sqrt{2}} \cos(f(\theta)) |\uparrow\uparrow\rangle + \frac{1}{2} |\uparrow\downarrow\rangle + \frac{1}{2} |\downarrow\uparrow\rangle + \frac{1}{\sqrt{2}} \sin(f(\theta)) |\downarrow\downarrow\rangle \quad (22)$$

and f is some real function of θ . It is easy to verify that eq. (21) satisfies the constraints eq. (15). As a functional of f , the probability of biasing the outcome to 0 (or 1) then reads

$$P_{0*}^{(2)} = \frac{1}{64} \left(12 \cos(2f(\theta)) \cos(\theta) + 2 \sin(2f(\theta)) \sin^2(\theta) + \cos(f(\theta)) (12\sqrt{2} \sin(\theta) + \sin(2\theta)) \right. \\ \left. + \sin(f(\theta)) (12\sqrt{2} \sin(\theta) - \sin(2\theta)) - \cos(2\theta) + 37 \right). \quad (23)$$

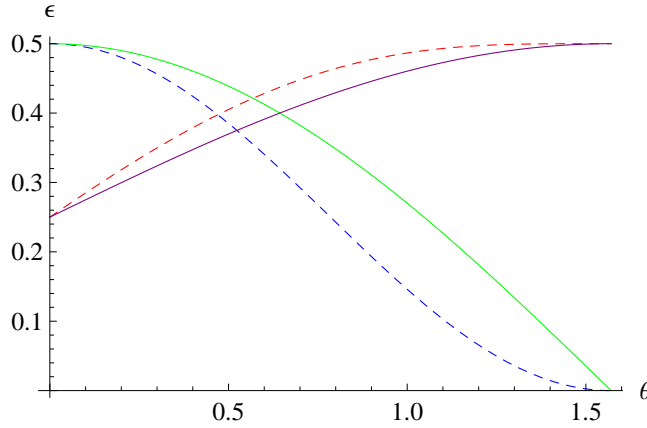


Figure 3: Maximal biases as a function of θ for $N \leq 2$ qubits. The dashed (solid) decaying curve depicts Alice's bias for $N = 2$ ($N = 1$) and the dashed (solid) rising curve depicts Bob's bias for $N = 2$ ($N = 1$).

For $\theta \simeq 26.92^\circ$ $P_{0*}^{(2)}$ is maximized for $f \simeq 0.1177$ equaling 0.8975 as anticipated.

We see that while Alice's maximal bias decreases with the increase in the number of qubits, Bob's maximal bias increases as we go from one to two qubits (see Fig. 2). For a greater number of qubits, numerical based SDP evidence indicates the bias in the fair scenario continue to decrease with the increase in the number of qubits (Bob's bias increases), but at an increasingly slower rate. We were able to carry out numerics for up to six qubits, and obtained $P_F^{(3)} \simeq 0.8967$, $P_F^{(4)} = 0.8962$, $P_F^{(5)} \simeq 89.60$, $P_F^{(6)} \simeq 0.8958$ (in the later case $\theta \simeq 15.89^\circ$).

VI. CONCLUSION

It is possible to overcome the problem of losses in quantum CF. A loss-tolerant CF protocol has the property that its bias remains unchanged even if we allow for it to be restarted whenever losses occur. However, this robustness seems to come at a price. Berlin *et al.*'s loss-tolerant SCF protocol achieves a relatively high bias of 0.4. In this paper, by presenting a family of loss-tolerant SCF protocols, we were able to show that Berlin *et al.*'s result can be improved upon. Utilizing a single qubit we reproduced their result, while utilizing a pair of qubits we obtained a bias of 0.3975. SDP based numerical evidence indicates that the bias continues to decrease as the number of qubits is increased, but at a rapidly decreasing rate.

In future work it should be interesting to determine the theoretical limits on loss-tolerant CF protocols. Specifically, can Kitaev's bound be saturated by a loss-tolerant SCF protocol? If not, what is the bound on loss-tolerant SCF protocols? Furthermore, is it possible to introduce a loss-tolerant WCF protocol? Two main difficulties are apparent. First, at the end of a WCF protocol the losing party usually verifies the outcome by measuring a quantum system that has been kept in a quantum memory storage. Hence, in this scenario the losing party can always avoid losing by claiming to have lost the stored system. Second, the number of rounds of communication required to realize a CF protocol with a bias of ϵ is of the order of $\Omega(\log \log \epsilon^{-1})$. In particular, to achieve a loss-tolerant WCF protocol with an arbitrarily small bias will require the protocol to be impervious to losses occurring at any round, implying that a dishonest party must not be capable of (probabilistically) inferring whether it is going to win or lose at any round before the last.

Acknowledgments

We wish to thank Stefano Pironio for helpful discussions and acknowledge the support of the European Commission under the Integrated Project Qubit Applications (QAP), funded by the IST Directorate (Contract no. 015848). In addition, N. Aharon also acknowledges the support of the Binational Science Foundation and The Wolfson Family Charitable Trust (Grant number 32/08). S. Massar and J. Silman also acknowledge the support of the Inter-University Attraction Poles Programme (Belgian Science Policy) under Project IAP-P6/10 (Photonics@be).

Appendix A

Here we prove that Π_p can be set equal to the identity (see remark below eq. (8)), and we prove the constraints on primal problem, eq. (14).

Recall that

$$\sum_{\{\mathbf{b}\}} \sum_{\{\mathbf{r} | \bigoplus_i r_i = c\}} M_{0c}^{\mathbf{r}\mathbf{b}} = \Pi_p. \quad (\text{A1})$$

We would like to show that upon summation all Pauli basis vectors composed of one or more of the $\sigma_x^{(i)}$ or $\sigma_y^{(i)}$ vanish. To see this, we note for every element in the sum $M_{0c}^{\mathbf{r}\mathbf{b}}$ there is another element $M_{0c}^{\mathbf{r}'\mathbf{b}'}$, such that $b'_j = b_j \oplus \delta_{ij}$. Algebraically, this second element is identical to the first except that in its Pauli basis expansion the coefficient of every basis vector composed of either $\sigma_x^{(i)}$ or $\sigma_y^{(i)}$ has the opposite sign, so that upon summation they cancel each other. See eqs. (10) and (11).

It remains to show that the sum of all Pauli basis vectors composed solely of one or more of the $\sigma_z^{(i)}$ and identity operators vanish. We note that for every element in the sum $M_{0c}^{\mathbf{r}\mathbf{b}}$ there is another element $M_{0c}^{\mathbf{r}'\mathbf{b}'}$, such that $r'_k = r_k \oplus \delta_{ik} \oplus \delta_{jk}$ with $i \neq j$. This second element is identical to the first except that in its Pauli basis expansion the coefficients of basis vectors composed of either $\sigma_z^{(i)}$ or $\sigma_z^{(j)}$ (and identity operators), but not both, have opposite signs. See eqs. (10) and (11). The vanishing of basis vectors composed of both $\sigma_z^{(i)}$ and $\sigma_z^{(j)}$ (and identity operators), but not $\bigotimes_{i=1}^N \sigma_z^{(i)}$, then follows from repeating this argument for all possible pairs of indices k and $l \neq k$. Hence, upon summation all Pauli basis vectors composed of one or more of the $\sigma_z^{(i)}$, except $\bigotimes_{i=1}^N \sigma_z^{(i)}$, vanish, and it follows that

$$\sum_{\{\mathbf{b}\}} \sum_{\{\mathbf{r} | \bigoplus_i r_i = c\}} M_{0c}^{\mathbf{r}\mathbf{b}} = \alpha \mathbb{1} + \gamma \bigotimes_{i=1}^N \sigma_z^{(i)}. \quad (\text{A2})$$

However, from eq. (11) we have that

$$\sum_{\{\mathbf{b}\}} \sum_{\{\mathbf{r} | \bigoplus_i r_i = c \oplus 1\}} M_{0c \oplus 1}^{\mathbf{r}\mathbf{b}} = \alpha \mathbb{1} - \gamma \bigotimes_{i=1}^N \sigma_z^{(i)}. \quad (\text{A3})$$

Since both eqs. (A2) and (A3) must be equal, the coefficient of $\bigotimes_{i=1}^N \sigma_z^{(i)}$ must vanish and Π_p is seen to be proportional to the identity. This implies that Bob learns nothing from his first POVM with elements Π_p and Π_{rs} , since both elements are proportional to the identity. So that without loss of generality we can take Π_p equal to the identity.

Finally, since the sum is composed of $2^{2N-1} 2^N \times 2^N$ -dimensional matrices, and since in its Pauli basis expansion each matrix admits the same coefficient for the identity, it follows that $2^{N-1} \text{Tr}(M_{0c}^{\mathbf{r}\mathbf{b}}) = 1$. Together, these last remarks imply the constraints in the SDP eq. (14).

-
- [1] M. Blum, in *Advances in Cryptology: A Report on CRYPTO 81* (1982).
 - [2] J. Kilian, in *Proceedings of the 20th Annual ACM Symposium on the Theory of Computing* (1988).
 - [3] D. Aharonov, A. Ta-Shma, U. Vazirani and A.C. Yao, in *Proceedings of the 32nd Annual ACM Symposium on the Theory of Computing* (2000).
 - [4] R.W. Spekkens and T. Rudolph, *Quantum Inform. Compu.* **2**, 66 (2002).
 - [5] A. Ambainis, in *Proceedings of the 33rd Annual ACM Symposium on the Theory of Computing* (2001).
 - [6] R.W. Spekkens and T. Rudolph, *Phys. Rev. A* **65**, 012310 (2001).
 - [7] A. Kitaev, unpublished. The proof is reproduced in [14].
 - [8] A. Chailloux and I. Kerenidis, arXiv:0904.1511 [quant-ph].
 - [9] C. Mochon, arXiv:0711.4114 [quant-ph].
 - [10] R.W. Spekkens and T. Rudolph, *Phys. Rev. Lett.* **89**, 227901 (2002).
 - [11] L. Goldenberg, L. Vaidman and S. Wiesner, *Phys. Rev. Lett.* **82**, 3356 (1999).
 - [12] C. Mochon, in *45th Symposium on Foundations of Computer Science* (2004).
 - [13] C. Mochon, *Phys. Rev. A* **72**, 022341 (2005).
 - [14] A. Ambainis, H. Buhrman, Y. Dodis and H. Röhrig, in *Proceedings of the 19th IEEE Annual Conference on Computational Complexity* (2004).
 - [15] J. Barrett and S. Massar, *Phys. Rev. A* **69**, 022322 (2004).
 - [16] J. Barrett and S. Massar, *Phys. Rev. A* **70**, 052310 (2004).

- [17] N. Aharon and J. Silman, New J. Phys. **12**, 033027 (2010).
- [18] M. Ganz, arXiv:0910.4952 [quant-ph].
- [19] G. Berlín, G. Brassard, F. Bussi eres and N. Godbout, Phys. Rev. A **80**, 062321 (2009).
- [20] G. Berl n, G. Brassard, F. Bussi eres, N. Godbout, J.A. Slater and W. Tittel, arXiv:0904.3946 [quant-ph].
- [21] A.T. Nguyen, J. Frison, K. Phan Huy and S. Massar, New J. Phys. **10**, 083037 (2008).
- [22] C.H. Bennett and G. Brassard, in *Proceedings of the 1984 IEEE International Conference on Computers, Systems and Signal Processing* (1984).
- [23] L. Vandenberghe and S. Boyd, *Convex Optimization* (Cambridge University Press, 2004).